

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
MARSHALL DIVISION**

TQP DEVELOPMENT, LLC,

*Plaintiff,*

v.

1-800-FLOWERS.COM, INC., et al.,

*Defendants.*

§  
§  
§  
§  
§  
§  
§  
§  
§

Case No. 2:11-CV-248-JRG

**ORDER**

Before the Court is the briefing on Newegg’s Rule 50(b) Motion for Judgment as a Matter of Law (Dkt. No. 436); Newegg’s Notice of Supplemental Authority (Dkt. No. 447); Newegg’s Notice of Subsequent Authority (Dkt. No. 450); Newegg’s Second Notice of Subsequent Authority (Dkt. No. 453); and TQP’s Response to Newegg’s Supplements (Dkt. No. 452.) For the reasons set forth below, Newegg’s Motion for Judgment as a Matter of Law is GRANTED as to non-infringement.

**BACKGROUND**

The Court held a jury trial in this case and the jury entered a verdict on November 25, 2013. At the time of trial, the asserted claims of U.S. Patent No. 5,412,730 (“’730 Patent”)—the sole patent-in-suit—were Claims 1, 6, 8, and 9. The Jury returned a verdict that the asserted claims were not invalid; that the asserted claims were directly infringed and that Newegg had induced its customers to infringe; and \$ 2.3 MM as a “sum of money, if paid now in cash” that “would fairly and reasonably compensate TQP for its damages resulting from Newegg’s infringement of the ’730 Patent.”<sup>1</sup> (Dkt. No. 407 (“Verdict”).)

---

<sup>1</sup> At trial TQP had asserted that it, if damages were awarded, the proper amount was \$ 5.1 MM. Newegg did not present its own expert testimony on damages.

After trial Newegg filed a Motion for Judgment as a Matter of Law (Dkt. No. 436) and a Motion for a New Trial (Dkt. No. 437). Briefing on these motions concluded on April 4, 2014. After briefing completed on its Motion for Judgment as a Matter of Law, Newegg filed three supplements, the last of which was filed on July 25, 2014. On June 4, 2014, Newegg filed its Notice of Supplemental Authority (“First Supplement”). (Dkt. No. 447.) On June 30, 2014, Newegg filed its Notice of Subsequent Authority (“Second Supplement”). (Dkt. No. 450.) On July 8, 2014, the Court ordered TQP to respond to Newegg’s supplements. (Dkt. No. 451.) On July 25, 2014, Newegg filed a Second Notice of Subsequent Authority (“Third Supplement”). (Dkt. No. 453.) On August 7, 2014, the Court issued a Memorandum Opinion and Order on an issue of Newegg’s Motion for Judgment Based on the Defense of Laches. (Dkt. No. 454.)

Newegg’s Notice of Subsequent Authority (Dkt. No. 450) informed the Court of a June 20, 2014 ruling in a related case—*TQP Development, LLC v. Intuit Inc.*, Case No. 2:12-cv-180 (hereinafter (“*Intuit Case*”)), Dkt. No. 192 (hereinafter “*Intuit SJ Order*”))—in which the judge in that case (J. Bryson) revised his earlier construction of a term in the ’730 Patent and granted summary judgment of non-infringement.<sup>2</sup> In this case, TQP responded that it would be filing a Motion for Reconsideration of the grant of non-infringement in the *Intuit Case*. Newegg’s Third Supplement (Dkt. No. 453) informed the Court that a Motion for Reconsideration of the *Intuit SJ Order* had been denied: Dkt. No. 203 in the *Intuit Case* (hereinafter “*Intuit SJ Reconsideration Order*”) filed on July 23, 2014. On August 21, 2014, TQP filed a Notice of Appeal to the United States Court of Appeals for the Federal Circuit in the *Intuit Case*, which was docketed on August 26, 2014, appealing, among other rulings, the *Intuit SJ Order* and the *Intuit SJ Reconsideration Order*. On October 2, 2014, TQP’s appeal of the orders in the *Intuit Case* was dismissed.

---

<sup>2</sup> Testimony from this trial comprised part of the evidence submitted in the summary judgment briefing in *Intuit*.

Newegg's Notice of Supplemental Authority (Dkt. No. 447) submitted the Supreme Court's, June 2, 2014, decision in *Limelight Networks, Inc. v. Akamai Technologies, Inc., et al.*, 134 S.Ct. 2111 (2014). Newegg asserted that the Supreme Court "rejected the rule of *Akamai Techs., Inc. v. Limelight Networks, Inc.*, 692 F. 3d 1301, 1305-07, 1318 (2012) (en banc) that a party can be liable for active inducement of infringement of a method claim under 35 U.S.C. § 271(b) when that party is not responsible for the performance of the entire method such that it would be a direct infringer under 35 U.S.C. § 271(a)." *Id.* The *Limelight* decision was reversed and remanded. *Id.* On May 13, 2015, the decision on remand issued in *Akamai Technologies, Inc. et al., v. Limelight Networks, Inc.*, 786 F.3d 899 (Fed. Cir. 2015). A petition for en banc rehearing was filed on June 25, 2015, in that case.

### **The '730 Patent**

The '730 Patent lists a sole inventor—Michael F. Jones—and is entitled "Encrypted data transmission system employing means for randomly altering the encryption keys." (Dkt. No. 348 at 12.) The '730 Patent was filed on April 23, 1992 (the patent is a continuation in part of Ser. No. 418,178, which was filed on, Oct. 6, 1989, and subsequently abandoned) and issued on May 2, 1995. (*Id.*) The '730 Patent was originally assigned to Telequip Corporation of Hollis, New Hampshire. (*Id.*)

The asserted claims—Claims 1, 6, 8, and 9—of the '730 patent are as follows (the Parties' identifications of specific limitations (e.g., a, b, c) have been added for Claim 1):

**Claim 1.** [(a)] A method for transmitting data comprising a sequence of blocks in encrypted form over a communication link from a transmitter to a receiver comprising, in combination, the steps of:

[(b)] providing a seed value to both said transmitter and receiver,

[(c)] generating a first sequence of pseudo-random key values based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link,

[(d)] encrypting the data sent over said link at said transmitter in accordance with said first sequence,

[(e)] generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said predetermined characteristic of said data transmitted over said link such that said first and second sequences are identical to one another a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link,

[(f)] and decrypting the data sent over said link at said receiver in accordance with said second sequence.

**Claim 6.** The method of claim 1, wherein said provided seed value is one of a number of different seed values for a plurality of remote locations with which secure communication is required.

**Claim 8.** The method of claim 1, further comprising:

Associating different ones of seed values with each of a plurality of remote locations with which secured communication is required.

**Claim 9.** The method of any one of claims 3, 4, 5, 6, 7, or 8, further comprising:

Adding error control information to the data sent over said link, wherein the error control information is added prior to transmitting the data over said link.

### **The Accused Technology**

The technology accused of infringement in this case relates to secure communications and the World Wide Web. Specifically the accused technology concerns secure Hypertext Transfer Protocol (“HTTP”) communications, commonly referred to as “HTTPS.” HTTPS, which one might commonly see as part of the address in a web browser (e.g. “https://”), requires

one of two additional protocols: called Secure Socket Layer (“SSL”) or Transport Layer Security (“TLS”).<sup>3</sup> (11/21 PM Tr. (Stubblebine) 63:16-21.) TQP accuses Newegg’s use of either the combination of the SSL protocol and the RC4 cipher or the combination of the TLS protocol and the RC4 symmetric key encryption algorithm in Newegg’s external facing servers. (11/19 AM Tr. 61:17-23; 128:10-129:13; *see also* 11/21 PM Tr. (Stubblebine) 26:1-12 (describing RC4).) TQP asserts that “SSL and TLS are essentially interchangeable” but that “SSL doesn’t infringe by itself” and “RC4 doesn’t meet all the limitations by itself”; “it’s only the combination” of SSL with RC4 that infringes. (*Id.*; *Id.* 61:25-62:2; 130:1-4.)

The SSL and TLS protocols, speaking generally, define an ordered process for establishing secure communications. As TQP’s expert Dr. Jager testified, the secure communications of the patent are “set up when the customer puts in this URL” and “goes to the website,” at which point “the customer’s computer [is] led through . . . a process by the website in order to setup [] secure communication.” (11/19 PM Tr. (Jager) at 133:6-23; *see also* 11/21 PM Tr. (Stubblebine) 25:7-25 (describing SSL handshake).) Said another way, SSL and TLS are the protocols that “lead[] the customer’s computer through the negotiation.” (*Id.*) “And as part of that negotiation, an encryption algorithm [(in this case RC4) is] selected to protect the secrecy of the data sent between the website and their computer.” Specifically, the SSL and TLS protocols provide that the server selects the particular encryption algorithm—also referred to as a “cipher suite” in this case—that will be used from among the various encryption algorithms listed by the client as part a particular message called the ClientHello. (*Id.* 139:7-20.) As a

---

<sup>3</sup> SSL and TLS are standardized protocols with published specifications that have different versions. (11/19 AM Tr. (Jager) 129:14-17; 130:21-25.) The evidence presented at trial concerned Newegg’s use of SSL version 3 and TLS version 1. (*Id.* at 129:18-25; 11/21 PM Tr. (Stubblebine) 77:13-17; 78:10-14.)

concrete example of this process, Dr. Jager testified how, Newegg's website, as part of the SSL or TLS protocols, selects the RC4 cipher suite from among a number of other choices:

Q. Okay. And what happens after the customer accesses Newegg's HTTP website and sends this ClientHello message?

A. Right. So the ClientHello is followed by another message called the server hello from the -- this will be from the Newegg website. And the server hello provides one line, it says cipher suite and has one entry for that.

And so this is the cipher suite selected by what's called the server in the TLS protocol and the Newegg websites are the servers in the -- in the TLS protocol.

Q. Okay.

A. And so we will use TLS and we will use RC4 for this session.

Q. Okay. And where in the list of cipher suites that you provided is that?

A. Well, there were 27, and this one is No. 19, if I'm not mistaken. I can't see it from here. Well, yeah, I can. I can't read it very well. Anyway, so this is the 19th one. So what's happening is that the Client -- the browser wants to work with a lot of different websites, and so they're going to support a number of default cipher suites so they can -- they can connect securely with a number of different websites.

And they'll provide a set of these, and in -- in this protocol, the server is the one that selects the cipher suite. And so it will just select whichever one is the first one that the server wants to use, if it's supported in the list that's provided by the -- the browser.

(11/19 PM Tr. (Jager) at 140:25-142:6; 142:17-20; *see also* 11/21 PM (Stubblebine) 39:27-41:4 (discussing the handshake process and cipher suite selection); 71:10-19.)

Dr. Jager testified that "the website deployer chooses how -- what protocol [(e.g., SSL or TLS)] you need to use to connect to that website," and that "[i]f you don't use the protocol that they selected, then you won't be able to use their website." (*Id.* 134:4-8.) In other words, a "customer computer cannot connect to the Newegg [https.secure.newegg.com](https://secure.newegg.com) website if it doesn't

use SSL or TLS.” (11/19 PM Tr. (Jager) at 137:1-7; *see also* 11/21 PM (Stubblebine) 64:8-21 (describing that Newegg makes the decision to require that those connecting to its websites use HTTPS).) However, as Dr. Stubblebine—Newegg’s expert—testified, if a user’s list of available cipher suites did not include RC4, then the server would simply select another cipher. (11/21 PM Tr. (Stubblebine) 43:14-45:21.)

### **APPLICABLE LAW**

Upon a party’s renewed motion for judgment as a matter of law following a jury verdict, the Court asks whether “the state of proof is such that reasonable and impartial minds could reach the conclusion the jury expressed in its verdict.” Fed. R. Civ. P. 50(b); *Am. Home Assur. Co. v. United Space Alliance*, 378 F.3d 482, 487 (5th Cir. 2004). “The grant or denial of a motion for judgment as a matter of law is a procedural issue not unique to patent law, reviewed under the law of the regional circuit in which the appeal from the district court would usually lie.” *Finisar Corp. v. DirectTV Group, Inc.*, 523 F.3d 1323, 1332 (Fed. Cir. 2008). “A JMOL may only be granted when, ‘viewing the evidence in the light most favorable to the verdict, the evidence points so strongly and overwhelmingly in favor of one party that the court believes that reasonable jurors could not arrive at any contrary conclusion.’” *Versata Software, Inc. v. SAP Am., Inc.*, 717 F.3d 1255, 1261 (Fed. Cir. 2013) (quoting *Dresser-Rand Co. v. Virtual Automation, Inc.*, 361 F.3d 831, 838 (5th Cir. 2004)).

Under Fifth Circuit law, a court is “especially deferential” to a jury’s verdict, and will not reverse the jury’s findings unless they are not supported by substantial evidence. *Baisden v. I’m Ready Productions, Inc.*, 693 F.3d 491, 499 (5th Cir. 2012). “Substantial evidence is defined as evidence of such quality and weight that reasonable and fair-minded men in the exercise of impartial judgment might reach different conclusions.” *Threlkeld v. Total Petroleum, Inc.*, 211 F.3d 887, 891 (5th Cir. 2000). A motion for judgment as a matter of law must be denied “unless

the facts and inferences point so strongly and overwhelmingly in the movant's favor that reasonable jurors could not reach a contrary conclusion." *Baisden* 393 F.3d at 498 (citation omitted). Furthermore, "[t]here must be more than a mere scintilla of evidence in the record to prevent judgment as a matter of law in favor of the movant." *Arismendez v. Nightingale Home Health Care, Inc.*, 493 F.3d 602, 606 (5th Cir. 2007).

In evaluating a motion for judgment as a matter of law, a court must "draw all reasonable inferences in the light most favorable to the verdict and cannot substitute other inferences that [the court] might regard as more reasonable." *E.E.O.C. v. Boh Bros. Const. Co., L.L.C.*, 731 F.3d 444, 451 (5th Cir. 2013) (citation omitted). However, "[c]redibility determinations, the weighing of the evidence, and the drawing of legitimate inferences from the facts are jury functions, not those of a judge." *Reeves v. Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 150 (2000). "[T]he court should give credence to the evidence favoring the nonmovant as well as that 'evidence supporting the moving party that is uncontradicted and unimpeached, at least to the extent that that evidence comes from disinterested witnesses.'" *Id.* at 151 (citation omitted).

## ANALYSIS

Newegg's Motion challenges all aspects of the verdict—direct infringement, active inducement of infringement, validity, and damages—under F.R.C.P. 50(b).

### Direct Infringement

1. **The "a new key value in the first and second sequence is used each time a predetermined number of blocks have been sent over the communications link" limitation.**

Newegg asserts that TQP failed to prove the "have been sent" limitation of Claim 1(e) (contained in the construction of the bolded portion below):

generating a second sequence of pseudo-random key values based on said seed value at said receiver, each new key value in said sequence being produced at a time dependent upon said



predetermined characteristic of said data transmitted over said link such that said first and second sequences are identical to one another **a new one of said key values in said first and said second sequences being produced each time a predetermined number of said blocks are transmitted over said link.**

The Court instructed the jury that the **bolded** limitation (above) had the following construction:

a new key value in the first and second sequence is used each time a predetermined number of blocks have been sent from the transmitter over the communication link.

You should note, as to the determination of whether “a predetermined number of said blocks” have been “transmitted over said link,” the claim explicitly refers to transmission, not to encryption or to some other step of preparing for transmission.

(Dkt. No. 421 at 33:23-34:9.) Generally, Newegg asserts that, in its system, “a new key value” is generated before the “predetermined number of blocks have been sent from the transmitter over the communication link,” and that such a system cannot infringe the claims because the “predetermined number of block” must “have been sent” before “a new key value” is generated. (Mot. at 4.) Generally, TQP asserts that the language of Claim 1(e) refers to action at the receiver (not at the transmitter) and that there is no requirement in the claims that, as to the transmitter, the “predetermined number of block” must “have been sent” before “a new key value” is generated. (Resp. at 5 n.4.)

As a predicate to the evidence presented on the “have been sent” limitation (discussed below), the Parties also focused on the “predetermined number of blocks” limitation, which generally defines the temporal interval of the claims (as will be seen below). At trial, Dr. Jager—TQP’s expert—repeatedly testified that the “predetermined number of blocks” requirement of Claim Element 1(e) was met in Newegg’s system by a one block unit of 8 bits (or one byte). (11/20 AM Tr. (Jager) 23:2-24:15; *see also* 25:19-26:4; 11/19 PM Tr. (Jager)

148:5-22.) Dr. Jager further testified the block counter in Newegg's system was built into the RC4 cipher. (11/20 AM Tr. (Jager) 63:14-24.)

Having reviewed the trial record, the Court believes the following pieces of testimony provide a foundation for understanding the evidence underlying the dispute as to the "have been sent" limitation. At trial, Dr. Jager provided the following description of how Element 1(e) was met by Newegg's system:

Q. Okay. So let's look at the Court's construction of the last part of Element 1(e). How does Newegg's use of SSL and RC4 meet this?

A. Well, my understanding of this construction is it's stating that -- that a new key value in the first and second sequence is used each time a predetermined number of blocks have been sent from -- from the transmitter -- you can't see it all -- over the communication link.

And this is the Court's construction. The -- you can see we were defining the term predetermined characteristic to mean predetermined number of blocks.

So this is requiring that some number of blocks in RC4 -- one block is the number of blocks is -- is the predetermined characteristic.

In addition, the way I think about -- the way I understand this is that we're requiring a new key value in the first and second sequence.

Now, we're -- we're using symmetric key cryptography here so the key value has to be the same; we've restricted the sequences to be the same; but we also must ensure that encryption on a particular block is done with the same key value as decryption.

At this point, we're at claim Element 1(e) requiring that a new key value -- the same key value, one value -- in the first and second sequences is used.

So it has to be -- it's already -- it's already been used in the first sequence, but we're requiring that the same key value be used in both sequences at this point in Claim Element 1(e).

So let me show you how I -- how I envision this -- how I think about this. So we have the key values in the sequence. We're

producing key value based on the predetermined characteristic in the transmitter.

This key value encrypts a block of ciphertext. The next key value will be used to – to encrypt the next block of ciphertext. These are transmitted.

So -- so the -- the same new key value has to be used in -- in both the first and second sequence for the decryption to come off properly. If you use a different key value, you're not going to decrypt the data.

So here, when the block arrives, the same new key value is used also in the second sequence. So you have to use the same key value to decrypt the data so that the -- the invention works.

(11/20 AM Tr. (Jager) at 20:12-22:9.) Dr. Jager also provided the following clarification to his testimony:

Now, there's some additional constraints on -- in Claim 1(e) about the -- the relationship; for example, between the sequences. So here the bolded part says the first and second sequences are identical. So if there are differences in the first and second sequence, then we won't be able to decrypt the data properly and get our proper plain text back.

And as was mentioned earlier this morning using this pseudo-random number generator, if you have the same seed value, you'll produce the same sequence of numbers

So this requires explicitly that the first and second sequences are identical to one another.

(11/19 PM Tr. (Jager) at 125:21-126:8.)

Outside of his description of how Claim 1(e) was infringed, Dr. Jager was also questioned on specific examples. Dr. Jager testified that a set of 20 encrypted blocks (20 one-byte blocks) would be encrypted, using different keys, and would likely be placed into a common packet before being sent:

Q. For 2 -- I'm sorry -- for 160 bytes, do you know whether that's -- in the Newegg system, whether that's transmitted all at once or

whether it's transmitted in 160 different pieces being sent one at a time over the Internet?

A. Well, so SSL and TLS don't determine that. But my -- my experience is that that's smaller than the maximum packet size, so - - so likely it would be transmitted in one.

Q. All at one time?

A. Yeah.

Q. So in that instance in the Newegg system, an encryption key -- a new encryption key is used to encrypt Byte No. 2 before encrypted Byte No. 1 is sent over the Internet, correct?

A. That's true, but that -- that isn't -- that isn't related to the claim language, as I understand -- or the claim construction, as I understand it.

(11/20 AM Tr. (Jager) At 54:22-55:14.) Dr. Jager was questioned by Newegg's counsel as to whether he believed each encrypted block had to "have been sent" before the next block was encrypted:

Q. (By Mr. Baldauf) Looking at the claim constructions in this case, I believe you were asked whether there was anything in the claims that required when a sequence of blocks could be sent.

Did you say that there was nothing in the claims that limited that?

A. When the blocks are -- nothing that limits when blocks can be sent?

Q. With respect to when a key value is used, do you agree with me that the claim requires that a new key value can be used only when the previously encrypted block has been transmitted over the communication link?

A. I see. Yeah.

So what I was referring to was the transmitter -- that there wasn't a limit on when -- constraint on when the transmitter could send the block.

But there is a limitation, as you point out here, that the new key value, which is the same value, and needs to be the same value in the transmitter/receiver for things to work.

So the new key value in the first and second sequence is used -- at this time the block has been sent because this is part of 1(e), which is describing what's going on in the receiver. It's saying the receiver has to use the same key value as the transmitter.

Q. But this construction requires -- has been sent from the transmitter over the communication link, correct?

A. Yes.

Q. So we're talking about when blocks are being sent from the transmitter to the receiver, correct?

A. No. What we're talking about -- the fact that they have been sent.

Q. Correct, have been sent.

A. Yes.

Q. Okay. Thank you.

(11/20 AM Tr. (Jager) at 122:24-124:9.) TQP's counsel then reexamined Dr. Jager on this point:

Q. (By Mr. Giza) Opposing counsel has asked you about the Court's construction of the last part of Element 1(e), and he just showed you the construction.

Can you explain to the jury how you understand this construction is met using your animation?

A. Yes. So the construction requires a new key value in the first and second sequences. So this means that the same key value has to be used from the first and second sequences. We don't use the same key value in the first sequence and the second sequence.

Then we're not going to encrypt and decrypt with the same key. So we're not going to get the data that we sent in the first place.

So the animation -- if I turn it on -- there it goes -- shows -- no. I turned it off. Okay. There we go -- shows a new key value.

Key Value 1 in the first sequence is used, and then I believe -- and then for the next predetermined number of blocks, Key Value 2 is used. So they're used in the first sequence.

....

Q. So now the blocks have been transmitted to the receiver. That's where this limitation is referring to, right?

A. Yes. The blocks now have been sent from the transmitter over the communication link, and so the predetermined number of blocks is satisfied. The key value now in the first and second sequence is used when the predetermined number of blocks have been sent from the transmitter over the communication link.

Q. Okay. And what happens with the -- the next block?

A. I don't think it shows it.

Q. Okay. But with -- when the next block comes to the decryptor, what's produced?

A. The -- the second key -- well, so the second key value will be produced.

So now the second key value in the first second sequences is used each time a predetermined number of blocks have been sent from the transmitter over the communication link.

(11/20 AM Tr. (Jager) at 125:1-126:21.) Newegg's counsel then again asked whether, in Dr. Jager's understanding, the second block was encrypted with the second key before the first encrypted block had been sent:

Q. And what you have in this animation -- you show that we've got one block, the green block, and two blocks -- the second block, the blue block -- block, they've been encrypted already, correct?

A. As is shown here, yes.

Q. And they've each been encrypted using a different key value, correct?

A. Block 1 was encrypted with a different key value than Block 2, yes.

Q. So Block 2, the blue block, is being encrypted using a new key value before Block 1 has been transmitted across the communication link, correct?

A. That's correct.

Q. Thank you.

(11/20 AM Tr. (Jager) at 130:11-24.)

Dr. Subblebine—Newegg’s expert—testified that under TQP’s theory—as presented above by Dr. Jager—Newegg could not infringe, since, under Dr. Subblebine’s understanding of the claims, the claims require that the encrypted block must be sent before the second block is encrypted. (11/21 PM Tr. (Stubblebine) 32:11-33:24; 36:2-17.) Dr. Subblebine testified that, in Newegg’s system, many encrypted blocks are placed into the same Internet packet before that packet is sent over the Internet. (*Id.* 37:14-39:6; 88:1-20; 91:24-92:23.) Dr. Stubblebine clarified that the claims did allow for multiple blocks to be sent with the same key (e.g., where the number of blocks was greater than 1), but that Newegg had asserted that the accused number of blocks was 1. (*Id.* 53:22-54:6; 56:5-10.)

Condensing the evidence discussed above, the Parties are in substantive agreement that, in Newegg’s system—or in SSL/TLS in combination with RC4—a first block that has been encrypted (“Block 1”) with a first key (“Key 1”) is not transmitted before a second block (“Block 2”) is encrypted with a second key (“Key 2”). Instead, as discussed above, Block 1 is placed into a packet to be transmitted along with a number of other blocks, each of which is encrypted with a different key, and is transmitted at some undefined time. The Parties’ substantive dispute is not what evidence was presented at trial but whether Newegg’s system infringes the claims.

The Court concludes that under either Newegg’s or TQP’s interpretation there was not a showing of substantial evidence that the claim limitation is infringed.<sup>4</sup> The Court’s conclusion is centered on the lack of substantial evidence showing a direct causal (or temporal) link between

---

<sup>4</sup> The Court therefore does not determine whether either interpretation is solely correct or whether the claim supports both interpretations. The Court does note that J. Bryson, having been presented with closely related arguments concerning the same limitation of the ’730 Patent, concluded that the ambiguity could be resolved. *See Intuit SJ Order; Intuit SJ Reconsideration Order.*

the generation of a new key and either the transmission or receipt of the encrypted block, either in Newegg's system, in SSL in combination with RC4, or in TLS in combination with RC4.<sup>5</sup> The Court finds that the claim limitation clearly requires such a causal (or temporal) link (e.g., "a new key value is used . . . each time a predetermined number of blocks have been sent from the transmitter"). The Court finds that this causal (or temporal) link is not simply a requirement that the same key be used in encryption and decryption, essentially a restatement of using a key, but is a required causal (or temporal) link between specific elements of the limitation.

The substantial evidence presented at trial was that, in the accused system, the RC4 cipher processes blocks, producing a new key with each block. The Court finds no substantial evidence that this action of the RC4 cipher is directly coupled to (or directly depends on) when, if, or the manner in which enciphered blocks are transmitted or received. In other words, regardless of whether the claim is viewed from the perspective of the transmitter or the receiver, the Court finds no substantial evidence that "a new key value . . . is used each time a predetermined number of blocks have been sent from the transmitter over the communication link." For example, if viewed from the perspective of the transmitter, the evidence is that new keys continue to be generated as each block is processed regardless of whether or not each already enciphered block has been transmitted. As but another example, if viewed from the perspective of the receiver, there is no substantial evidence that the generation of new keys at the transmitter is tied to whether or not a packet of enciphered blocks has been received (or is in the process of being received) by the receiver.

The Court's conclusions regarding the lack of a causal link between the generation of a new key and either the transmission or receipt of the encrypted block is further strengthened by

---

<sup>5</sup> At trial TQP, did not present evidence under the doctrine of equivalents. The Court therefore need not determine whether Newegg's system falls within an equivalent of the claims.



other evidence that was presented. For example, TQP asserted both that it was only the combination of RC4 with SSL or TLS that infringed and that neither RC4, SSL, nor TLS infringed separately. The evidence presented at trial was also that RC4 was but one of a number of possible cipher suites that could be selected by Newegg's servers as part of the SSL or TLS protocols, and that even if RC4 was not present in the list of cipher suites (or was present but not selected), the SSL or TLS protocols would continue and would establish secure communications using another cipher suite. Such evidence indicates that SSL and TLS, in essence, operate independently of the particular cypher suite that is selected, strongly suggesting that the behavior of any particular cipher suite (e.g., RC4) is not coupled to TLS or SSL.

The Court finds that, regarding this specific limitation of Claim 1(e), the verdict of infringement is not supported by substantial evidence and that the “facts and inferences point so strongly and overwhelmingly in the movant's favor that reasonable jurors could not reach a contrary conclusion.” The Court reaches its conclusion after having “view[ed] the evidence in the light most favorable to the verdict” and “draw[ing] all reasonable inferences in the light most favorable to the verdict.” Accordingly, the Court finds as a matter of law that Newegg does not infringe element 1(e) of Claim 1 of the '730 Patent, and that, consequently, Newegg does not infringe Claim 1 of the '730 Patent. The Court therefore **VACATES** the Jury's verdict of infringement as to Claim 1 and hereby enters a verdict of no infringement as to Claim 1. As the remaining claims in suit—6, 8, and 9—which all depend upon Claim 1, the Court further **VACATES** the Jury's verdict of infringement as to Claims 6, 8, and 9 and hereby enters a verdict of no infringement as to those claims.

## **2. The “predetermined number of blocks” limitation.**

As discussed above, TQP presented evidence that the “predetermined number of blocks” was met by Newegg's system when it processed each one byte unit. Newegg briefly argues that

the—“predetermined number of blocks”—claim limitation cannot be met if the number of blocks is 1. The Court does not find support for Newegg’s position—that the “predetermined number of blocks” limitation requires two or more blocks.

**3. The “generating a first sequence of pseudo-random key values based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link” limitation.**

Newegg briefly argues that the key value must be “exclusively based on the seed value” according to the Court’s construction of this limitation. (Mot. at 10.) In other words, Newegg argues that if the key value is “based on” anything other than the seed value, the claims cannot be infringed. The Court does not find support for Newegg’s position—that “based on said seed value” means “exclusively based on the seed value.

**4. Direction or control**

The parties do not dispute that some of the accused steps are performed by Newegg’s customers’ computers. However, the Parties do substantively dispute whether there is substantial evidence that Newegg directs or controls these activities. *See e.g., Akamai Technologies, Inc. et al., v. Limelight Networks, Inc.*, 786 F.3d 899 (Fed. Cir. 2015). As the Court has already determined that there is no infringement of the asserted claims, the Court does not reach this issue.

**Induced Infringement**

After post-trial briefing completed in this case, the Supreme Court issued its ruling in *Limelight Networks, Inc. v. Akamai Technologies, Inc.*, 134 S. Ct. 2111 (2014). As discussed above, the Parties submitted supplemental briefing. In *Limelight* the Supreme Court held that “inducement liability may arise if, but only if, there is direct infringement.” *Limelight* 134 S. Ct. at 2117 (citing *Aro Mfg. Co. v. Convertible Top Replacement Co.*, 365 U.S. 336, 341 (1961))

(internal quotation omitted). The Court recognized that “*Aro* addressed contributory infringement under § 271(c), rather than inducement of infringement under § 271(b)” but saw “no basis to distinguish for these purposes between the two.” *Id.* n.3.

Accordingly, since the Court has found that there is no direct infringement, the Court finds that there can be no liability for induced infringement as a matter of law. The Jury’s verdict of induced infringement is therefore **VACATED** and the Court hereby enters a verdict of no induced infringement.

### CONCLUSION

For the reasons set forth above, the Court **GRANTS** Newegg’s Rule 50(b) Motion for Judgment as a Matter of Law (Dkt. No. 436) as to the issue of infringement. The Court hereby **VACATES** the Jury’s verdicts of direct and induced infringement as to Claims 1, 6, 8, and 9 of the ’730 Patent and enters a verdict of NO DIRECT INFRINGEMENT and NO INDUCED INFRINGEMENT as a matter of law as to those claims. The Court **CARRIES** Newegg’s Rule 50(b) Motion for Judgment as a Matter of Law on the remaining issues of invalidity and damages.

While the Court does not ordinarily comment on such matters, the Court feels it should briefly address the Petition for Writ of Mandamus that Newegg filed on July 6, 2015 (Dkt. No. 459.) The Court is aware that more time has passed since the briefing has been complete on Newegg’s Motion than is optimal.<sup>6</sup> However, although approximately 20 months have passed

---

<sup>6</sup> After Newegg’s Petition for Mandamus was docketed in this case, the Court, among other actions, immediately asked the District Clerk to investigate why its systems had failed in this case, both to understand the issue and to, hopefully, determine a way to prevent such an occurrence in future. District Clerk David Maland forwarded his findings to the Court:

I am responding to your inquiry of July 8th as to why defendant Newegg’s post-trial motions have not been appearing on the 6 month CJRA pending motion report. Upon inquiry, it was discovered that an order staying Case No. 2:11-cv-428, a case with a similar number, was inadvertently docketed in the instant case

since the trial in this case, the time at which Newegg's Motion for JMOL was fully briefed and Newegg's Supplements were before the Court—the point in time where these matters typically would have been decided—was approximately 12 months ago. While Newegg did file an electronic notice with the Clerk's office during this time (approximately 8 months ago), this is the sole action that Newegg has taken. Never once in this time has counsel for Newegg directly contacted the Court's staff inquiring about this matter. How this situation could simultaneously be so prejudicial that a resort to mandamus might be considered while, at the same time, Newegg could not be troubled to pick up a phone and call the Court's staff is baffling.


Finally, the Court intends to address, by written opinions, the issues that it has carried within a reasonable time. The Court, like most courts, has a busy docket, which periodically may cause more time to pass in a particular case than is optimal. In the future, the Court suggests that the parties themselves would be better served (and costs reduced) if they elected not to shoot first and ask questions later.

---

on June 7, 2013 (docket entry #242 - see attached screen shot; erroneous order also attached). A note was made by the docket clerk at that time that the stay order was filed in error, but she neglected to lift the stay flag in the database. The bottom line is that a stay was created when the erroneous order was entered in this case and the stay flag remained in place until it was discovered and removed on July 8, 2015. This prevented any pending motions in this case from showing on your pending CJRA motions report during that time period.

Please accept my deepest apology for this situation. We have advised the deputy clerk in question of her error and have taken curative actions designed to avoid repetition of this kind of error. Please contact me if you have any questions.

**So ORDERED and SIGNED this 15th day of July, 2015.**

  
\_\_\_\_\_  
RODNEY GILSTRAP  
UNITED STATES DISTRICT JUDGE